



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,904	06/28/2001	Yves Louis Gabriel Audebert	L741.01105	1582

7590 02/01/2006
STEVENS, DAVIS, MILLER & MOSHER, LLP
Suite 850
1615 L Street, N.W.
Washington, DC 20036

EXAMINER

SHIFERAW, ELENI A

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 02/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/892,904

Applicant(s)

AUDEBERT ET AL.

Examiner

Eleni A. Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 October 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 38-61 is/are pending in the application.
- 4a) Of the above claim(s) 1-37 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 38-61 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date: _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 28, 2005 has been entered.
2. Claims 38-61 are presented for examination.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 38-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaliski, Burton S. (Kaliski, EP 0 807 911 A1) in view of Debry US. 6,314,521 B1.

Regarding claims 38 and 50, Kaliski teaches a personal security device (PSD)/method that generates a digital certificate, the PSD comprising:

a first encryption component that encrypts a unique device identifier (KSS) for the PSD (col. 8 lines 28; smart card/client) to produce an encrypted unique device identifier (col. 5 lines 33-35; *Time Stamp (TS) and secret session key (KSS), that is generated with device identifier's information, are encrypted using asymmetric key or*

server's/authenticator's/validator's public key);

a second encryption component that encrypts first contextual attributes of the PSD to produce encrypted first contextual attributes (claim 1 element e, and col. 5 lines 33-40; *encrypting TS using KSS/symmetric key);*

a first combiner that combines the encrypted unique device identifier (KSS), and the encrypted first contextual attributes for generating the digital certificate (col. 5 lines 24-41, fig. 4A element 36, and fig. 3A element 107 & 108; *concatenating KSS/TS, and KSS/TS with KSS(cert-C)), wherein*

the unique device identifier (KSS) and first contextual attributes are encrypted using different encryption keys (claim 10 element a and b; *KSS is encrypted with server's public key, and part of the certificate/TS is encrypted with symmetric key/KSS).*

Kaliski fails to teach:

A first encryption component that encrypts a **unique device identifier** for the PSD to produce an encrypted unique device identifier; and

a first combiner that combines the unique device identifier, the encrypted unique device identifier.

However Debry discloses a message digest and a digital signature authentication when a printer/card of cellular phone (col. 6 lines 12-17) sends a message to a server (col. 6 lines 33-51). The message comprising encrypted **serial number/unique card identifier** of the card and **clear/non-encrypted serial number/unique card identifier** of the card (abstract). The server authenticates the message by decrypting the encrypted serial number received and comparing the decrypted serial number with the non-encrypted serial number

received (claim 1 lines 9-30).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Debry within the system of Kaliski because they are analogous in message digest authentication of a card (Debry col. 3 lines 9-29 and col. 4 lines 23-39). One would have been motivated to incorporate the teachings, of combining and sending the clear device identifier and encrypted device identifier for authentication, to validate the identity and integrity of the device by comparing the locked identifier with the unlocked one.

Regarding claims 45 and 57, Kaliski teaches a host/method for validating a digital certificate that is received from a personal security device (PSD), the host comprising:

a first decryption component that decrypts an encrypted unique device identifier (decrypting KSS) for the PSD (claim 37; smart card/client), which is received in the digital certificate, to produce a decrypted unique device identifier (column 26 lines 6-10, and col. 20 lines 22-25; decrypting KSS using server's private key);

a second decryption component that decrypts encrypted first contextual attributes of the PSD, which are received in the digital certificate, to produce decrypted first contextual attributes (**claim 18 and col. 12 lines 48-49**, and col. 20 lines 28-30; *TS is encrypted with certificate using KSS/symmetric key*);

a second comparator that compares the decrypted first contextual attributes to reference attributes, which are known to the host, to determine a second match result (col. 9 lines 41-49; *comparing received and/or decrypted TS with stored/reference TS*); and

a validating component that validates a portion of the digital certificate if second match results both indicate a match (col. 9 lines 41-51 and fig. 3B element 209; *if TS match... authentic*).

Kaliski fails to disclose:

a first decryption component that decrypts an **encrypted unique device identifier**, which is received in the digital certificate, to produce a decrypted unique device identifier; and

a first comparator that compares the decrypted unique device identifier to a unique device identifier received in the digital certificate to determine a first match result and validate if match.

However Debry discloses:

a first decryption component that decrypts an **encrypted unique device identifier**, which is received in the digital certificate, to produce a decrypted unique device identifier (col. 12 lines 44-56; *decrypting the encrypted card identifier/serial number*); and

a first comparator that compares the decrypted unique device identifier to a unique device identifier received in the digital certificate to determine a first match result and validate if match (col. 12 lines 57-63, and abstract).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Debry within the system of Kaliski because they are analogous in message digest authentication of a card (Debry col. 3 lines 9-29 and col. 4 lines 23-39). One would have been motivated to incorporate the teachings, of combining and sending the clear device identifier and encrypted device

identifier for authentication, to validate the identity and integrity of the device by comparing the locked identifier with the unlocked one.

Regarding claims 39 and 51 Kaliski and Debry teach all the subject matter as described above. In addition the combination teaches the PSD/method further comprising:

a third encryption component that encrypts the combined encrypted first contextual attributes, encrypted unique device identifier (Kaliski col. 5 lines 37-41 and fig. 5 element 13; *TS and KSS are encrypted using symmetric key*), and unique device identifier to produce an encrypted message authentication code (MAC) (Debry col. 4 lines 32-36, and col. 14 lines 6-9); and

a second combiner that combines the encrypted MAC with the unique device identifier, the encrypted unique device identifier, and the encrypted first contextual attributes in the digital certificate (Kaliski col. 8 lines 46-55; *concatenating KSS/TS/encrypted certificate*, Debry col. 6 lines 52-57; *certificate is concatenated with digital signature and/or encrypted*). The rationale for combining are the same as claim 1 above.

Regarding claims 40-41, 44, 52-53, and 56 Kaliski and Debry teach all the subject matter as described above. In addition the combination teaches the PSD/method wherein:

the unique device identifier is encrypted with an asymmetric encryption key (col. 21 lines 35-41; *KSS encrypted using asymmetric*; and **encrypting a device name/identifier/serial number with public/private key is very well-known please see**

Aiello et al. US 6,496,808 B1 col. 8 lines 14-55);

the first contextual attributes are encrypted with a first symmetric encryption key (claim 18; *TS is encrypted with KSS*); and
the MAC is encrypted with a second symmetric encryption key (Kaliski col. 24 lines 22-27, and Debry col. 4 lines 32-36, and col. 14 lines 6-9). The rational for combining are the same as claim 45 above.

Regarding claims 42 and 54, Kaliski and Debry teach all the subject matter as described above. In addition the combination teaches the PSD/method wherein the first combiner combines second contextual attributes (col. 8 lines 12-25, and col. 6 lines 5-7; *CRL/expiration time*) of the PSD with the unique device identifier, the encrypted unique device identifier, and the encrypted first contextual attributes for generating the digital certificate (Kaliski claim 44, Debry col. 4 lines 32-36, col. 6 lines 36-44, and col. 14 lines 6-9; combines KSS, TS, signed card certificate, and Debry combines signed certificate, clear unique device identifier/SN, encrypted identifier...). The rational for combining are the same as claim 45 above.

Regarding claims 43 and 55, Kaliski and Debry teach all the subject matter as described above. In addition the combination teaches the PSD/method further comprising:

a third encryption component that encrypts the combined encrypted first contextual attributes, second contextual attributes (col. 8 lines 12-25, and col. 6 lines 5-7; *CRL/expiration time*), encrypted unique device identifier, and unique device identifier

to produce an encrypted message authentication code (MAC) (Kaliski col. 24 lines 22-27, and Debry col. 4 lines 32-36, and col. 14 lines 6-9); and

a second combiner that combines the encrypted MAC with the unique device identifier, the encrypted unique device identifier, the encrypted first contextual attributes, and the second contextual attributes in the digital certificate (Kaliski col. 24 lines 22-27, and Debry col. 4 lines 32-36, and col. 14 lines 6-9). The rationale for combining are the same as claim 1 above.

Regarding claims 46 and 58, Kaliski and Debry teach all the subject matter as described above. In addition the combination teaches the host/method further comprising:

a combiner that combines the encrypted first contextual attributes, the encrypted unique device identifier, and the unique device identifier to produce a message authentication code (MAC) (Kaliski claim 44, Debry col. 4 lines 32-36, col. 6 lines 36-44, and col. 14 lines 6-9; combines KSS, TS, signed card certificate, and Debry combines signed certificate, clear unique device identifier/SN, encrypted identifier...);

an encryption component that encrypts the MAC to generate an encrypted MAC (Kaliski col. 24 lines 22-27, and Debry col. 4 lines 32-36, and col. 14 lines 6-9); and

a third comparator that compares the generated encrypted MAC with an encrypted MAC received in the digital certificate to produce a third match result (Kaliski col. 9 lines 30-51, and Debry col. 7 lines 1-3 and col. 2 lines 65-col. 4 lines 39), wherein

the validating component validates the digital certificate if the first, second, and third match results all indicate a match (Kaliski col. 13 lines 7-24; *validates if the TS/second and MAC/third match*, and Debry col. 11 lines 9-27; *validates if the identifier in clear matches with encrypted/first*. The rationale for combining are the same as claim 45 above.

Regarding claims 47-48 and 59-60 Kaliski and Debry teach all the subject matter as described above. In addition the combination teaches the host/method wherein:

the unique identifier is decrypted with an asymmetric decryption key (Kaliski claim 1 element e; decrypting KSS using asymmetric key, and **decrypting a device name/identifier/serial number with public/private key is very well-known please see, Aiello et al. US 6,496,808 B1 col. 8 lines 14-55**);

the first contextual attributes are decrypted with a symmetric decryption key (Kaliski col. 20 lines 25-31; *TS is decrypted using symmetric key*); and

the MAC is encrypted with a symmetric encryption key (Kaliski col. 24 lines 22-27, and Debry col. 4 lines 32-36, and col. 14 lines 6-9). The rationale for combining are the same as claim 45 above.

Regarding claims 49 and 61 Kaliski and Debry teach all the subject matter as described above. In addition the combination teaches the host/method wherein the combiner combines second contextual attributes (col. 8 lines 12-25, and col. 6 lines 5-7; *CRL/expiration time*) of the PSD, which are received in the digital certificate,

with the unique device identifier, the encrypted unique device identifier, and the encrypted first contextual attributes to produce the MAC (Kaliski claim 44, Debry col. 4 lines 32-36, col. 6 lines 36-44, and col. 14 lines 6-9; combines KSS, TS, signed card certificate, and Debry combines signed certificate, clear unique device identifier/SN, encrypted identifier...). The rationale for combining are the same as claim 45 above.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

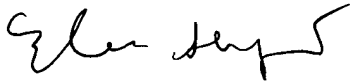
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.

Application/Control Number: 09/892,904

Page 11

Art Unit: 2136

A handwritten signature in black ink, appearing to read "Elen Jeyk".

January 4, 2006

A handwritten signature in black ink, appearing to read "Ayaz Sheikh".

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100